Introduction

Dans ce projet, je vais vous donner un guide étape par étape sur la façon de configurer et d'installer DVWA sur votre système Kali Linux.

Lorsque vous commencez en tant que testeur d'intrusion, vous aurez besoin d'un laboratoire de test d'intrusion pour tester vos compétences en pénétration. L'un de ces systèmes est la **Damn Vulnerable Web Application (DVWA).**

DVWA est une application Web vulnérable développée en utilisant PHP et MySQL qui permet aux pirates éthiques de tester leurs compétences en piratage et leurs outils de sécurité.

C'est également un excellent guide pour les développeurs Web professionnels ayant la sécurité à l'esprit. Ils peuvent l'utiliser pour apprendre quelles fonctionnalités d'une application Web sont faciles à exploiter. Certaines des vulnérabilités Web les plus courantes démontrées par cette application incluent Cross-Site Request Forgery (CSRF), l'inclusion de fichiers, l'injection SQL, les attaques Bruteforce, et bien plus encore.

Étape 1: Télécharger Damn Vulnerable Web Application (DVWA)

Pour commencer, nous devrons cloner le GitHub DVWA dans notre répertoire. C'est l'emplacement où les fichiers Localhost sont stockés dans les systèmes Linux. Lancez le Terminal et changez notre répertoire pour le répertoire /var/www/html avec la commande ci-dessous.`/var/www/html`

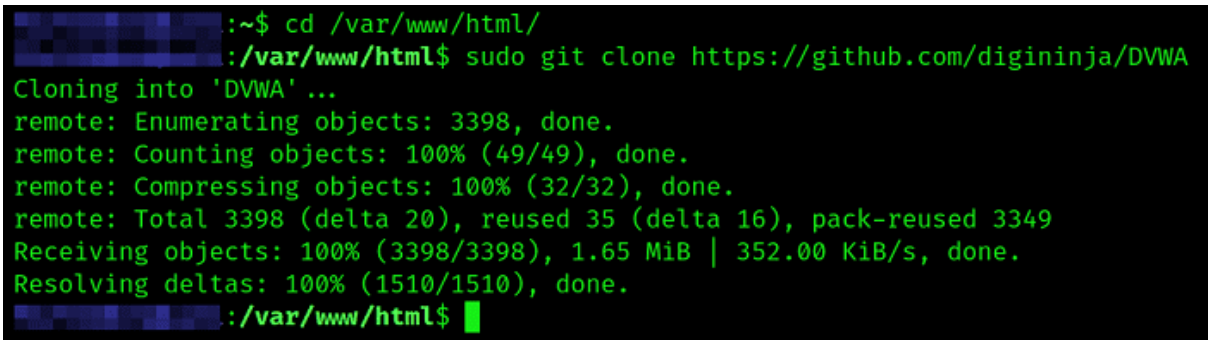
```
$ cd /var/www/html
```

Exemple de sortie :

Une fois dans ce répertoire, nous clonons le référentiel DVWA GitHub avec la commande ci-dessous.

```
$ sudo git clone https://github.com/digininja/DVWA
```

Exemple de sortie :



Après le clonage, nous pouvons renommer le dossier DVWA en . Ce n'est pas obligatoire, mais cela facilite le travail lors de l'exécution de plusieurs commandes.`dvwa`

```
$ sudo mv DVWA dvwa
```

Étape 2 : Configurer DVWA

Après avoir téléchargé le clonage DVWA dans notre répertoire, nous devons encore faire quelques configurations mineures. Pour commencer, définissons des autorisations de lecture, d'écriture et d'exécution sur le répertoire DVWA. Exécutez la commande ci-dessous.`/var/www/html`

```
$ chmod -R 777 dvwa/
```

Exemple de sortie :

Après avoir exécuté la commande avec succès, nous devons configurer l'utilisateur et le mot de passe requis pour accéder à la base de données. Changez de répertoire pour pointer vers le répertoire config avec la commande ci-dessous.

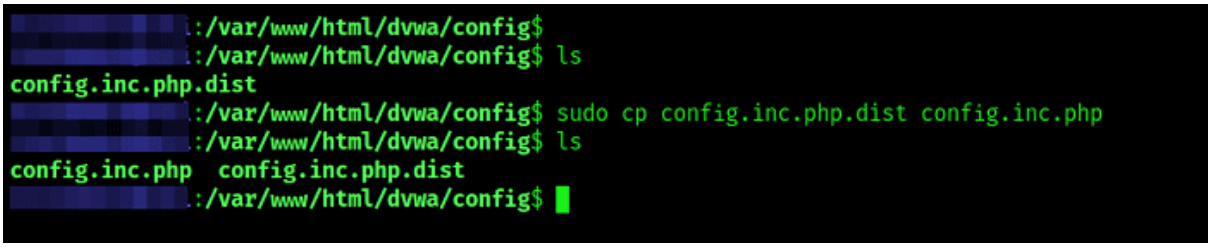
```
$ cd dvwa/config
```

Lorsque vous exécutez la commande **ls** pour afficher les fichiers à l'intérieur du répertoire, vous verrez le fichier. Il s'agit du fichier d'origine contenant les configurations par défaut. Nous ne le modifierons pas. Au lieu de cela, nous allons créer une copie de ce fichier appelé et le fichier original agira comme notre sauvegarde en cas de problème `config.inc.php.dist` `config.inc.php` `config.inc.php.dist`

Exécutez la commande ci-dessous.

```
sudo cp config.inc.php.dist config.inc.php
```

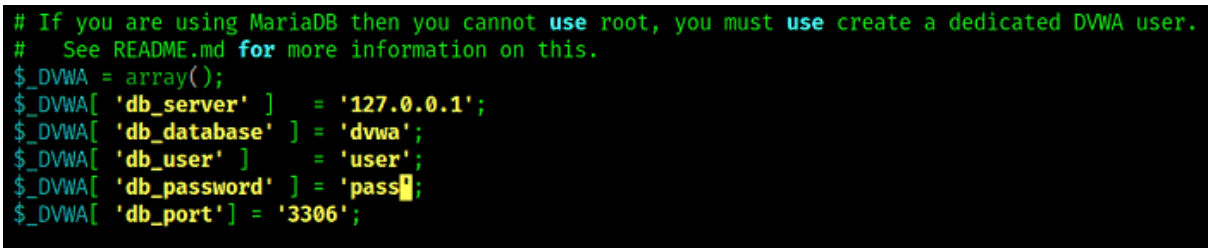
Exemple de sortie :



Exécutez la commande ci-dessous pour ouvrir le fichier nouvellement créé avec l'éditeur et apporter les modifications nécessaires, comme indiqué dans l'image ci-dessous. Nous définirons en tant qu'utilisateur et en tant que passe. N'hésitez pas à utiliser un nom d'utilisateur ou un mot de passe différent.`nano db_userdb_password`

```
$ sudo nano config.inc.php
```

Exemple de sortie :



Enregistrez le fichier (, puis) et Exit (Ctrl + X). Voilà! Nous avons terminé la configuration de l'application Web DVWA. Passons à autre chose et configurons la base de données (MySQL).

Étape 3: Installer MySQL sur Kali Linux

Par défaut, MySQL est préinstallé sur Kali Linux. Si ce n'est pas le cas pour vous ou si vous avez peut-être foiré avec MySQL, nous pouvons l'installer manuellement. Si vous avez travaillé avec des distributions basées sur Debian, MySQL est disponible en deux paquets :

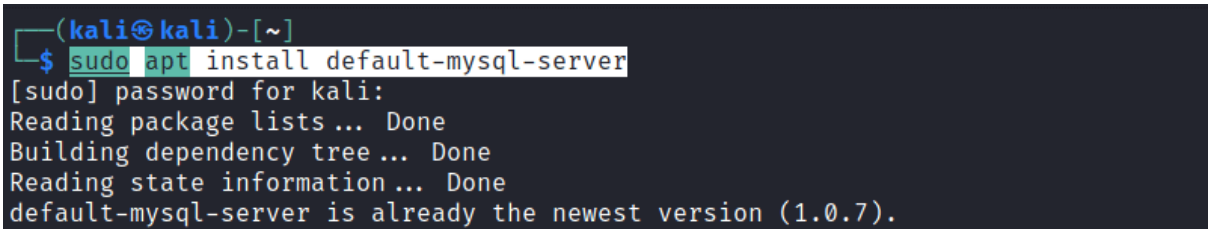
- serveur_mysql
- client_mysql

Dans notre cas, nous devrons installer le serveur mysql. Cependant, il y a un hic. Si vous essayez d'utiliser la commande apt install mysql-server, vous obtiendrez probablement l'erreur *« Le paquet mysql-server n'est pas disponible, mais est référencé par un autre paquet. E: Le paquet 'mysql-server' n'a pas de candidat à l'installation. »* C'est parce que le paquet mysql-server est référencé à default-mysql-server dans Kali

Linux et aussi dans la dernière version de Debian (Debian 10). Par conséquent, utilisez la commande ci-dessous:

```
sudo apt install default-mysql-server
```

Exemple de sortie :



Étape 4 : Configurer la base de données MySQL

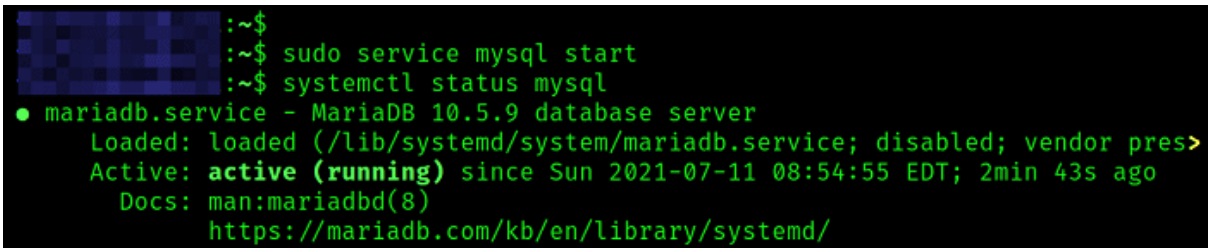
Démarrez le service Mysql avec la commande ci-dessous:

```
$ sudo service mysql start
```

Vous pouvez vérifier si le service est en cours d'exécution à l'aide de la commande ci-dessous.`systemctl status`

```
$ systemctl status mysql
```

Exemple de sortie :

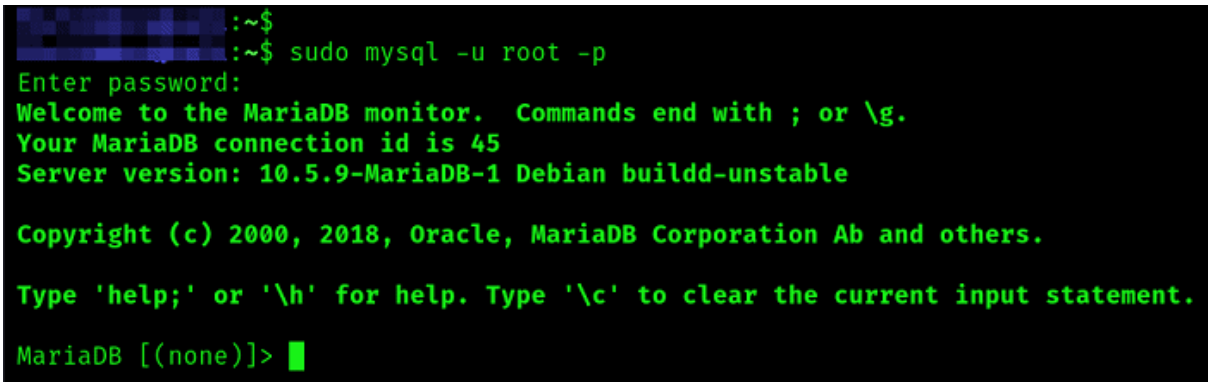


Connectez-vous à la base de données MySQL en utilisant la commande ci-dessous en tant que root. Si vous avez un autre nom défini pour le superutilisateur dans votre système, utilisez-le à la place de root.

```
$ sudo mysql -u root -p
```

Vous verrez une invite pour entrer le mot de passe. Appuyez simplement sur Entrée car nous n'avons défini aucun mot de passe. MySQL s'ouvrira, comme indiqué dans l'image

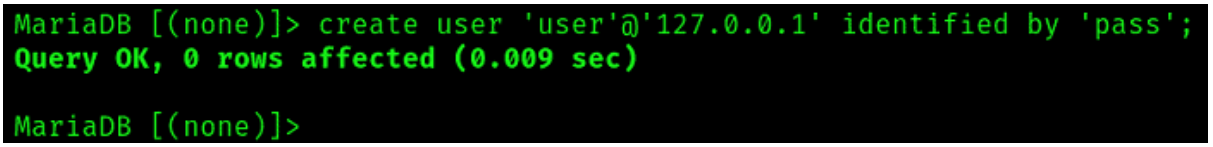
ci-dessous:



Nous allons créer un nouvel utilisateur avec le nom d'utilisateur et le mot de passe définis dans notre fichier de configuration d'application DVWA. Dans mon cas, le nom d'utilisateur était ',' et le mot de passe était '.' Le serveur que nous utilisons est Localhost (127.0.0.1). Utilisez la commande ci-dessous.`userpass`

```
create user 'user'@'127.0.0.1' identified by 'pass';
```

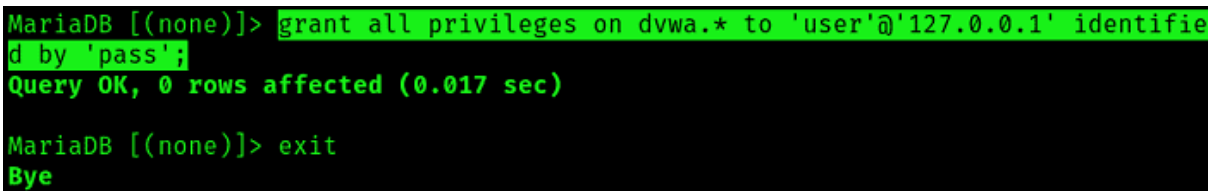
Exemple de sortie :



Nous devons accorder à ce nouvel utilisateur un privilège sur la base de données dvwa. Exécutez la commande ci-dessous.

```
grant all privileges on dvwa.* to 'user'@'127.0.0.1' identified by
'pass';
```

Jusqu'à présent, nous avons terminé la configuration de l'application DVWA et de la base de données MySQL. Tapez exit pour fermer la base de données.



Étape 5 : Installer PHP

PHP est installé dans Kali Linux. Cependant, si vous souhaitez installer une version particulière, vous pouvez le faire manuellement à partir du terminal, nous allons installer PHP 7.4 qui est la dernière version au moment de la rédaction. Suivez les étapes ci-dessous.

Tout d'abord, mettez à jour votre système et ajoutez le référentiel SURY PHP PPA en exécutant les commandes ci-dessous.

```
sudo apt update
```

```
sudo apt -y install lsb-release apt-transport-https ca-certificates
```

```
sudo wget -O /etc/apt/trusted.gpg.d/php.gpg https://packages.sury.org/php/apt.gpg
```

```
echo "deb https://packages.sury.org/php/ buster main" | sudo tee /etc/apt/sources.list.d/php.list
```

Exemple de sortie :

```
┌──(kali㉿kali)-[~]
└─$ echo "deb https://packages.sury.org/php/ buster main" | sudo tee /etc/apt/s
ources.list.d/php.list
deb https://packages.sury.org/php/ buster main

┌──(kali㉿kali)-[~]
└─$
```

Après avoir ajouté avec succès le référentiel, utilisez la commande ci-dessous pour installer PHP 7.4

```
sudo apt update
```

```
sudo apt install php7.4 -
```

Exemple de sortie :

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install php7.4
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  ettercap-common ettercap-graphical libluajit-5.1-2 libluajit-5.1-common
  python3-qrcode
```

Pour installer des extensions PHP supplémentaires, utilisez la syntaxe ci-dessous où xxx représente le nom de l'extension.

```
sudo apt install php7.4-xxx
```

```
sudo apt install php7.4-{cli,json,imap,bcmath,bz2,intl,gd,mbstring,mysql,zip}
```

Exemple de sortie :

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install php7.4-{cli,json,imap,bcmath,bz2,intl,gd,mbstring,mysql,zi
p}
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
php7.4-cli is already the newest version (7.4.21-1+deb11u1).
```

Étape 6 : Configurer le serveur Apache

Maintenant, nous devons configurer le serveur. Utilisez la commande ci-dessous pour modifier votre emplacement sur le Terminal afin qu'il pointe vers le répertoire.`/etc/php/7.3/apache2`

```
cogner

$ cd /etc/php/7.4/apache2
```

NOTE:

j'utilisais PHP version 7.4. Vous devrez peut-être confirmer votre version et la remplacer sur la commande. Utilisez la commande ci-dessous pour vérifier la version installée.

```
$ ls /etc/php
```

lorsque vous exécutez la commande ls, vous verrez un fichier appelé . C'est le fichier que nous allons éditer pour configurer notre serveur localhost. Utilisez la commande ci-dessous pour l'ouvrir à l'aide de l'éditeur nano.`/etc/php/7.4/apache2php.ini`

```
$ sudo nano php.ini
```

Faites défiler vers le bas et recherchez ces deux lignes : et . Réglez-les tous les deux sur On.

Enregistrez le fichier (, puis) et Exit ().

`allow_url_fopenallow_url_includeCtrl + OEnterCtrl + X`

```
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require to open URLs (like http:// or ftp://) as fil>
; http://php.net/allow-url-include
allow_url_include = On
```

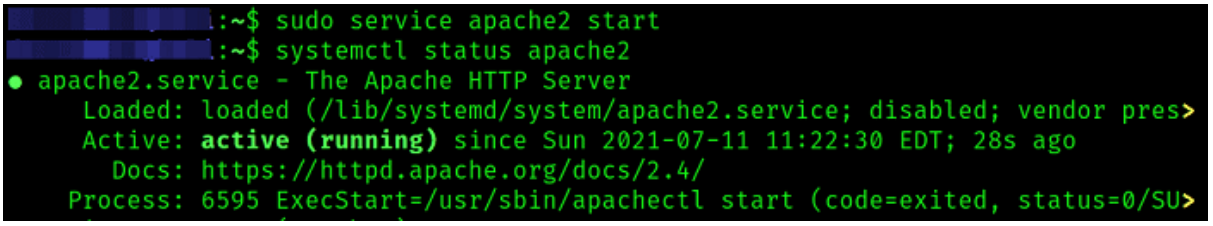
Démarrez le serveur Apache en utilisant la commande ci-dessous:

```
$ sudo service apache2 start
```

Pour vérifier si le service a démarré correctement, utilisez la commande status.

```
$ systemctl status apache2
```

Exemple de sortie :

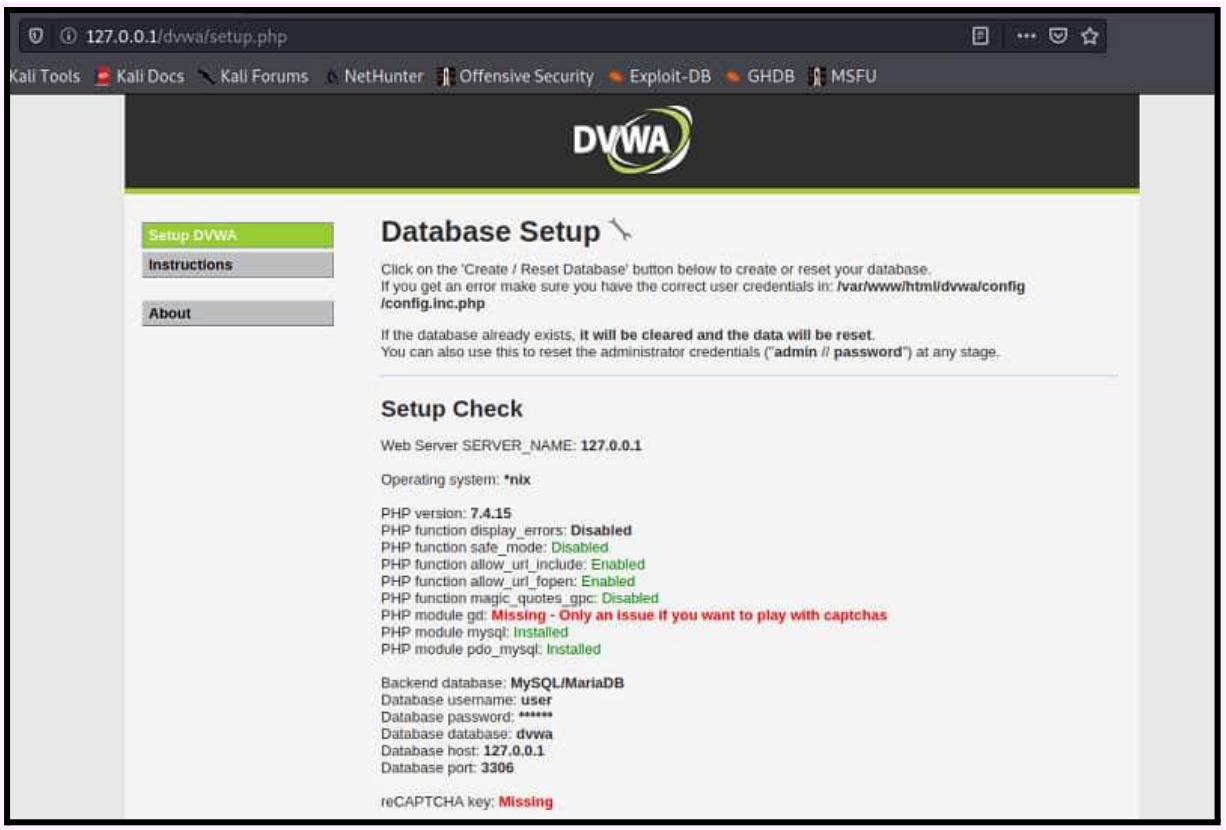


Étape 7: Accédez à DVWA sur votre navigateur

Voilà! Nous avons maintenant tout configuré et nous pouvons procéder au lancement de DVWA. Ouvrez votre navigateur et entrez l'URL :

```
http://127.0.0.1/dvwa/
```

Cela ouvrira la page Web comme indiqué dans l'image:`setup.php`

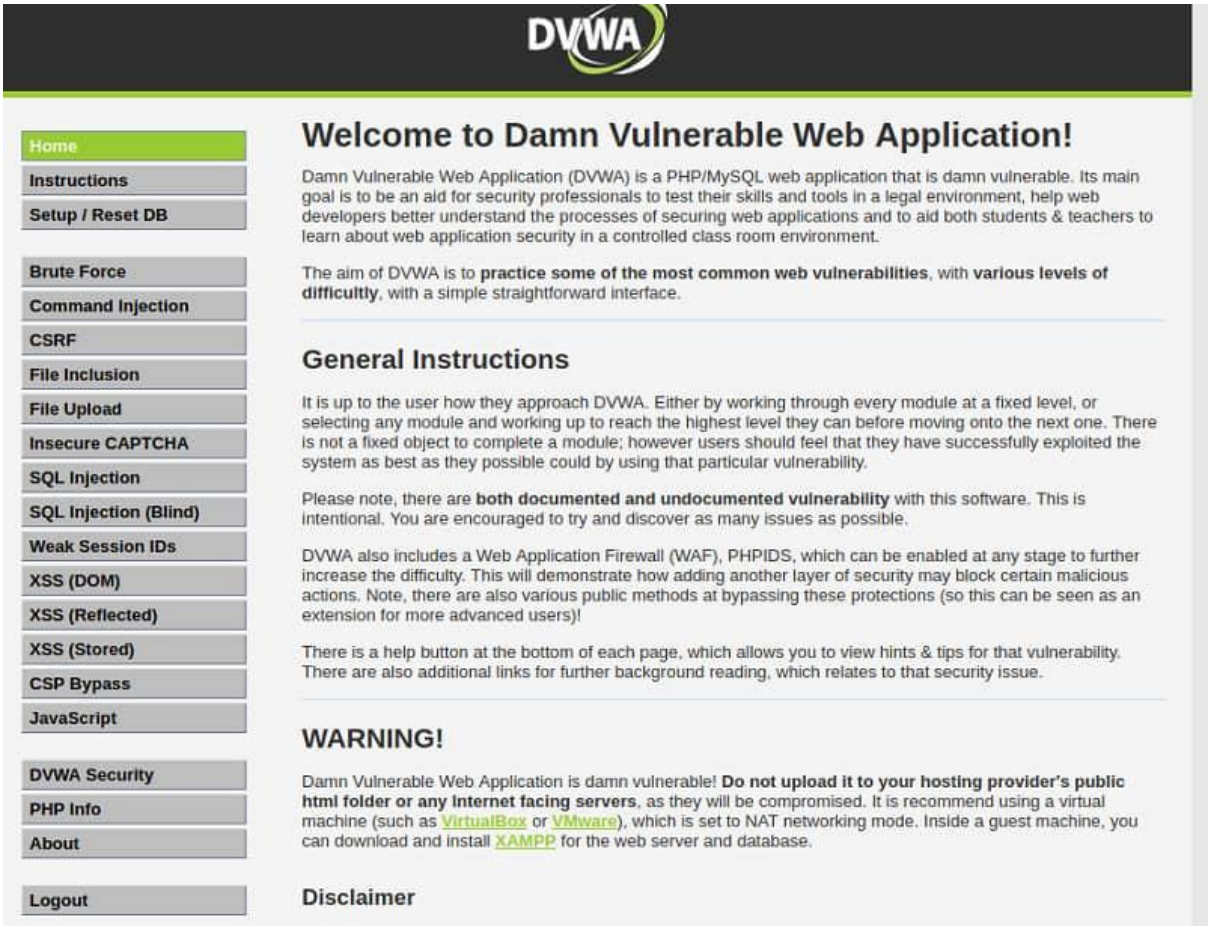


Vous pouvez voir les erreurs colorées en rouge comme dans l'image ci-dessus. Pas de panique ! Faites défiler vers le bas et cliquez sur le bouton Créer / Réinitialiser la base de données.

Cela créera et configurera la base de données. Après un certain temps, vous serez redirigé vers la page de connexion DVWA. Connectez-vous avec ces informations d'identification :

- Nom d'utilisateur - admin
- Mot de passe - mot de passe

Une fois connecté, vous verrez la page principale DVWA. Sur le panneau de gauche, nous avons les différents types d'attaques que vous pouvez exploiter et le bouton de sécurité DVWA qui vous permet de choisir le niveau de sécurité souhaité - Faible, Moyen, Haut ou Impossible.



Conclusion

DVWA est une excellente ressource pour les débutants qui débutent avec les tests d'intrusion et les experts. Tout ce que vous avez à faire est de modifier les niveaux de sécurité en fonction de vos compétences. N'hésitez pas à partager la vulnérabilité que vous avez trouvée intéressante à exploiter avec nos lecteurs dans la section commentaires.